

Re: DNS revers lookup and mail server

Source:

<http://www.tech-archive.net/Archive/Exchange/microsoft.public.exchange.connectivity/2005-06/msg00005.html>

- *From:* "Steve Carr" <scarrNOSPAMBastyr.edu>
 - *Date:* Tue, 31 May 2005 15:34:35 -0700
-

You have most of it right but need to check two things. It sounds like all external heading mail goes through your thrid-party filtering system. If this is true, is there a way to set the FQDN for it to match what you want it to be (for example, in Exchange, you can go to the SMTP virtual server settings (in ESM) and then go to the Delivery tab and then click on advanced and see what is listed under FQDN. There you could make it anything you want). If you can change it, make it mail1.mycorpdomain.com so that all things match. If you can't change it (we use the Symantec SMTP gateway and it can't do that even though we've requested this as an added feature), then you'll need to add an additional DNS record with exsvr1 pointing also to the firewall external IP so you have a match this way

Also, check to make sure the IP that the external mail servers are seeing is indeed the the external interface of the firewall (no 1-to-1 NAT for the exsvr1 machine, for example) so that all matches (it sounds like this is correct but wanted to be thorough).

I believe if you match the name your server uses to send mail to the Reverse DNS IP result you'll be good to go

"Rafal W." <RafalW@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:944A9693-A8FB-4A31-A880-63CE93D36A78@xxxxxxxxxxxxxxxxxxxx>

> I guess I need some clarification here; my understanding was that properly

> configured mail server should have as follow:

- > 1. Static public IP address
- > 2. MX record for it and
- > 3. PTR added by ISP so IP address of mx record can be resolved to FQDN

>

> A reverse DNS lookup takes the IP address that's trying to make the
> connection, and checks to see if there is a registered domain associated
with
> it.

>

> For example, if an incoming message claims to be coming from the
> 66.160.177.11 IP address, an ISP would look up the domain to see if it
> resolves to lyris.com. If it doesn't, the message may be a forgery-or, the
> hapless sender may not have a correct DNS entry. In either case, the
message

Re: DNS revers lookup and mail server

- > will most likely be identified as spam.
- >
- > And all it cares is domain name in this example lyris.com, even though PTR
- > returns mx1.lyris.com what counts is lyris.com. Yes? No?
- >
- > Here is the reason why I'm asking for:
- >
- > 1. sender email us at joe.user@xxxxxxxxxxxxxxxxxxxx
- > 2. email goes out and looking in external DNS for MX record for
- > mycorpdomain.com which is resolved to public IP x.x.x.x
- > 3. email is delivered to our domain
- > 4. Joe User respond to sender – email goes out and is reaching mail server
- > which does reverse lookup, so
- > 5. recipient mail server knows what IP address is trying to make
- connection
- > (in this example x.x.x.x) and knows that sender claims to be from (in
- this
- > example) mycorpdomain.com
- > 6. so recipient mail server takes connecting IP address and does reverse
- > lookup, as a result it gets mail1.mycorpdomain.com
- >
- > Message is bounced back with following reason:
- >
- > 550 Requested actions not taken – SMTP sender domain
- > (exsvr1.mycorpdomain.com) not found in the DNS
- >
- > Where exsvr1.mycorpdomain.com is our third party anti-virus/mail filtering
- > software between firewall and mail server, and the way is setup is that mx
- > record of mail1.mycorpdomain.com has public IP of x.x.x.x pointing to
- > external interface of the firewall which then is NATed and redirected to
- > internal exsvr1.mycordomian.com.
- >
- > I kind of can see how do they get this name (exsvr1.mycorpdomain.com) in
- > returned NDR because if you lookup header of incoming messages you see
- > something similar to:
- >
- > Received: from exsvr1.mycorpdomain.com ([x.x.x.x])
- > by their.mail.server.receipient_domain.com (SMSSMTP 4.1.4.30) with SMTP id
- > M2005052413322418434
- > for <user@xxxxxxxxxxxxxxxxxxxxxx>; Tue, 24 May 2005 13:32:24 -0500
- >
- > x.x.x.x is my public IP which (as described above) can be resolved to
- > mail1.mycorpdomian.com but not exsvr1..
- >
- > does this mean you need to have physical smtp/mail box named same as mx
- > record ?in my case I would either rename box or call ISP and change so
- > x.x.x.x has PTR resolved to exsvr1.mycorpdomain.com instead
- > mail1.mycorpdomain.com ???
- >
- > was I all this time wrong about how it works? I always though DNS reverse
- > lookup takes IP and check registered domain in this case mycorpdomain.com

Re: DNS revers lookup and mail server

>
> Can someone verify that?
>

.

-
- Prev by Date: [*Re: Solution Found*](#)
 - Next by Date: [*Exchange 2003 and WAN connectivity problems*](#)
 - Previous by thread: [*Re: Solution Found*](#)
 - Next by thread: [*Exchange 2003 and WAN connectivity problems*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)